Ignorance is Risk

Singapore SME Cyber Preparedness Report 2019

CHUBB®

Contents

Welcome

Mr Andrew Taylor,
Cyber Underwriting Manager,
Chubb Asia Pacific

Following Chubb's inaugural SME Cyber Preparedness Report for Singapore in 2018, we are delighted to bring you the second edition of this report.

As one of the world's largest cyber insurers, we believe this report is important for raising awareness of the issues that small and medium-sized enterprises (SMEs) face in managing cyber risk. In the coming years, cyber risk is forecast to cost global businesses substantially in lost revenue. With SMEs making up 99% of all businesses in Singapore, employing 65% of Singapore's workforce and accounting for 49% of the country's GDP[1], they will be hardest hit without good risk mitigation, incident response planning and consideration of cyber insurance.

As Singapore invests heavily in digitalisation to strive towards its Smart Nation goals, local SMEs will need to be more prepared. Going digital has its pros and cons. But SMEs face some harsh realities if they continue to harbour the many misconceptions and ignorance about cyber incidents as this survey shows - 60% of them are not aware of all the cyber threats they face, while 59% think that large corporations are more at risk of cyber attacks than SMEs.

We hope that you will find this report useful and the insights can contribute towards reducing cyber risk for SMEs in Singapore.

[1] https://www.singstat.gov.sg/-/media/Files/visualising_data/infographics/economy/singapore-economy22032018.pdf

Ignorance is Risk

Cyber Risk Landscape

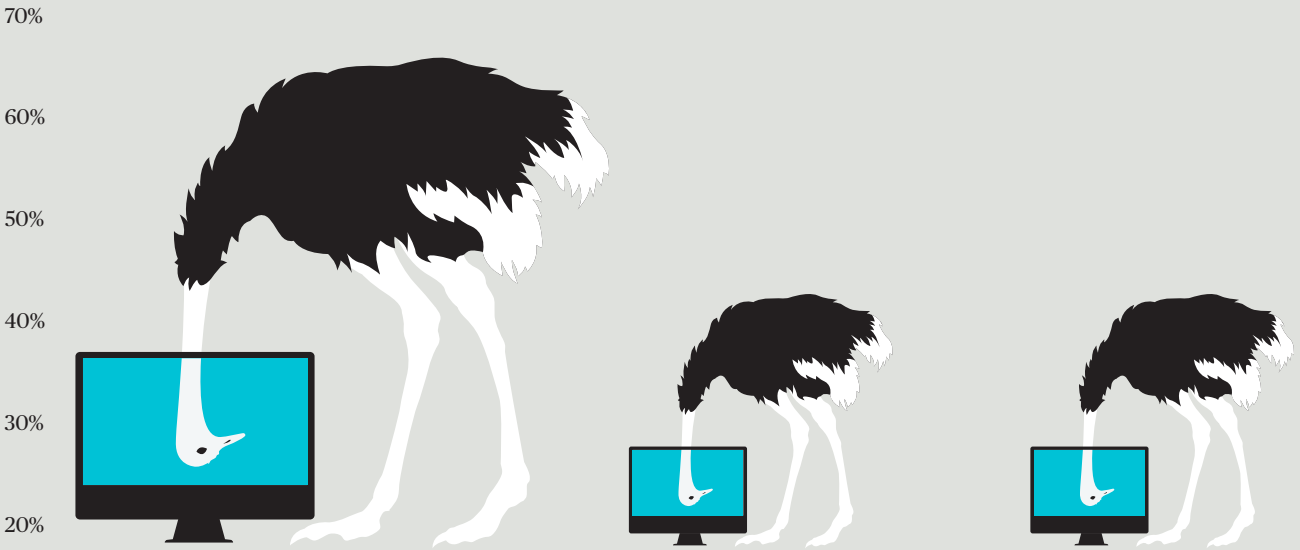
6,179 of cyber attacks occurred in Singapore in 2018, costing companies close to S$58 million in losses[2].

Singapore's government has responded with 13 new measures developed to protect citizens' personal data[3].

Digital Economy

Digital transformation is estimated to contribute US$10 billion to Singapore's GDP by 2021[4].

Key Survey Highlights



65%

of SMEs were victims of cyber incidents in the past year

40%

of all breaches involved customer records

40%

of SMEs surveyed do not have cyber risk insurance

[2] https://www.businessinsider.sg/businesses-in-singapore-lost-nearly-s58-million-to-cyber-attacks-last-year-csa-report/

[3] https://www.straitstimes.com/singapore/high-level-panel-rolls-out-13-cyber-security-measures-for-the-public-service-following

[4] https://news.microsoft.com/en-sg/2018/02/21/digital-transformation-contribute-us10-billion-singapore-gdp-2021/

Perception is Not Reality

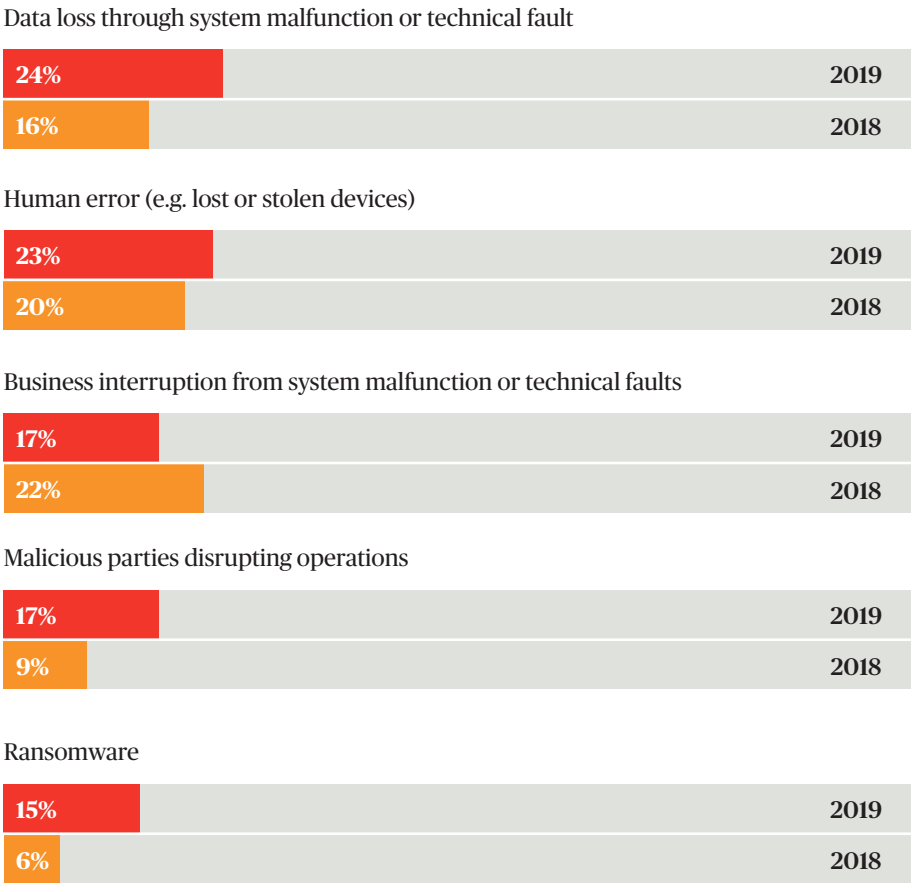
In this year's survey, nearly half (47%) of the respondents in Singapore say their organisation assumes it will never experience a cyber incident.

Yet, nearly two-thirds (65%) of Singapore SMEs reported experiencing a cyber incident in the past 12 months. This is an increase of 6% from 2018.

Two-thirds (67%) of the SME leaders who experienced an incident say that lessons had been learnt, and a similar incident was less likely in the future. Interestingly, more than half (54%) of leaders recognise that the incident was due to a risk they had already identified so this begs the question of why nothing was done to minimise the risk. Similar to 2018, there is a clear gap between perceived and actual preparedness.

Internal factors are still causing problems, with data loss caused by system malfunctions now occurring in 24% of incidents. Human error has also increased from 20% in 2018, being a factor in 23% of incidents in 2019. A small consolation, perhaps, is that business interruptions due to internal factors have dropped from 22% in 2018 to account for 17% of incidents in 2019.

Which types of cyber incidents did your business experience in the past 12 months?

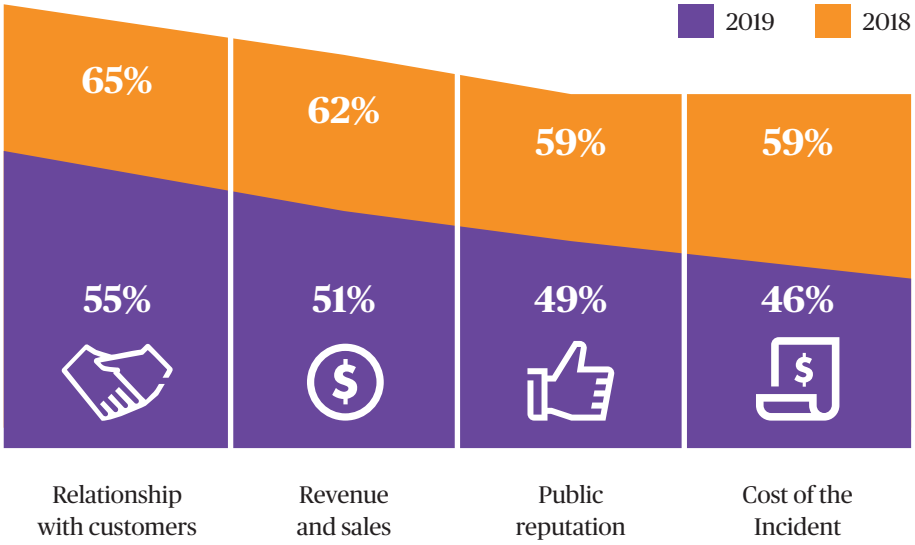


[5] https://www.singstat.gov.sg/-/media/Files/visualising_data/infographics/economy/singapore-economy22032018.pdf

Overconfidence Abounds

Despite the rise in cyber incidents over the past 12 months, SMEs seem less worried about the impact on their business, with significant drops across four key points of concern.

What are SMEs most worried about following a cyber incident?



This apparent lack of concern is worrying, as complacency leaves the door wide open for malicious attacks, future breaches and inadequate incident response.

This comes into sharp focus when we consider exactly what kind of data is accessed in a breach. In Singapore, 30% of the data files breached was email traffic of the senior team, followed by research and development data (24%), intellectual property data (23%) and financial performance data (23%). These are all commercially sensitive documents, which if exposed could impact business operations, reputation or the ability to compete.

While Singapore performed slightly better than other markets in protecting customer records, collectively this data was still accessed in 40% of all breaches. In 12% of incidents, the SME wasn't even aware of what data was breached.

Most Common Types of data files breached in the last 12 months	2019	2018
Email Traffic of Senior Team	30%	20%
Research and development (R&D) data	24%	11%
Intellectual property (IP) data	23%	11%
Financial performance	23%	15%
Employee records (including salary, performance reviews, personal details)	22%	15%

Uncoordinated, Unaware and Unprotected

The lack of concern around the impact of a data breach demonstrates a continued lack of understanding and awareness around cyber risk, particularly for SMEs.

Similar to last year's findings, 59% of SME leaders believe that large corporations are at more risk of cyber attacks than SMEs. Meanwhile, only 18% of SMEs are aware of all the cyber threats their business faces.

39% of leaders admit there isn't a consistent understanding within their organisation of what cyber risk means.

The chart below is a good indicator of why SMEs are such attractive targets for cyber criminals. If organisations remain uncoordinated, unaware and unprotected from digital threats, their data will remain a target for cyber criminals.

Case Study:
Ransomware attack

Industry:
Media

Annual Revenue:
S$30 million

Costs up to:
S$200,000

Approximately 20 of the company's servers containing client data relating to its business including artwork, historic and current project data were affected after a malicious file infected the servers over a weekend. With the servers down, the company was unable to fulfil their clients' orders.

The hacker(s) demanded two bitcoins to decrypt each server, increasing to four bitcoins per server if payment was not made within 48 hours. Following detection of the incident, the company contacted Chubb's Cyber Incident Response Hotline and spoke to the Incident Response Manager on the same day. A Chubb appointed IT forensic firm was deployed immediately.

With the assistance of the Chubb Incident Response Manager, the company and Chubb's appointed IT forensics firm were able to assist with a mitigation strategy by identifying less business-critical servers that could be restored from backups and negotiating the ransom amount.

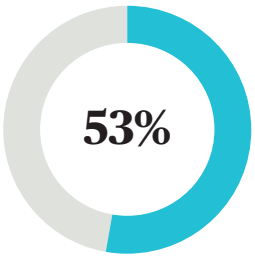
The response team removed the ransomware from the affected computers and also engaged a crisis management firm to assist with client communications.

A Cyber Risk Shared is a Cyber Risk Halved

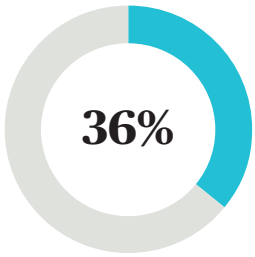
More than half of Singapore's SME leaders still see cyber risk management as an IT problem to solve, with 43% believing the head of IT (or equivalent) should hold ultimate responsibility for cyber risk management.

The IT department can only do so much to mitigate risk - and all their hard work is quickly undone, through simple mistakes such as if a careless employee was to leave a USB drive on the bus home.

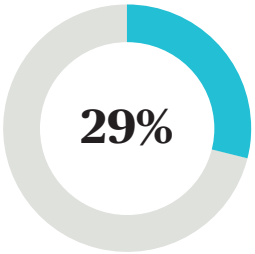
Indeed, SME leaders have a poor opinion of their employees' readiness against cyber incidents:



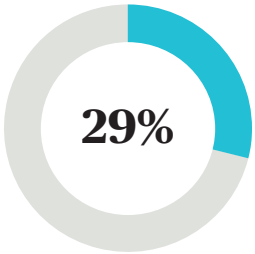
53% of SMEs are not confident that employees with access to sensitive data are fully aware of their data privacy responsibilities



36% say a principal challenge is employees neglecting their data protection responsibilities



29% of SMEs think employees are the weakest link in their cyber defence



29% say their employees have a poor understanding of the nature - and potential consequences - of the threats their business faces

This perception is not unfounded. After all, just over half (53%) of the cyber incidents that SMEs suffered in the past 12 months were caused by employees - either through administrative or clerical errors (30%) or through the loss or theft of a company device such as a laptop or USB drive (23%).

However, placing the blame solely on employees is not the answer. Fortunately, SME leaders are beginning to recognise the importance of better training in cyber risk management, with 58% identifying it as an important next step. Almost half (45%) also recognise that there should be clearer communication from the management to employees about the importance of cyber security.

Case Study: Ransomware attack

Industry:
Construction

Annual revenue approximately:
S$5 million

Costs up to:
S$500,000

A construction company that outsourced its IT operations suffered a ransomware attack because an employee clicked a malicious email link, causing the company's customer and project data to be encrypted.

The ransomware infected local hard drives and data that was backed up online. Without access to the digital records, the company could not operate its business as usual. Due to the failed attempts to negotiate with the extortionist, additional costs were incurred to re-construct and re-enter customer project records. This resulted in significant downtime and major loss incurred to the business.

Reducing the Risk with Insurance

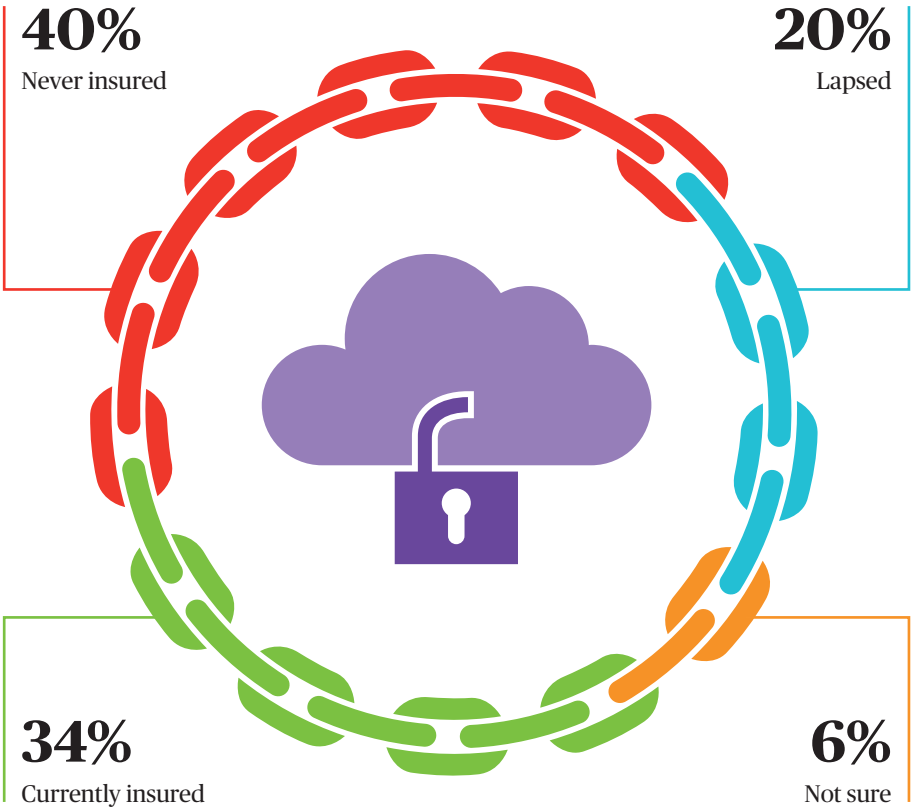
A serious cyber attack has the potential to do far more reputational and operational damage to a business than a tangible and recognisable incident, such as burglary or arson. While more businesses are getting smarter about this, far too many businesses remain uninsured against cyber risk.

60% of respondents in this year's survey say they believe insurance has a role to play in protecting against cyber risk, yet only 34% of SMEs are currently insured. 18% took up cyber insurance following a cyber incident to protect against future threats.

A further 40% of SMEs chose not to purchase cyber risk insurance either before or after an incident, while 20% had let their cover lapse over the last 12 months. 6% were unsure whether they had cover or not.

Of the additional services that insurers can offer when responding to an incident, SMEs saw good value in regulatory advice (58%) and assistance with speed of incident response (56%) from their insurer.

Cyber Risk Insurance Coverage Among SMEs



Dwelling on the Downside

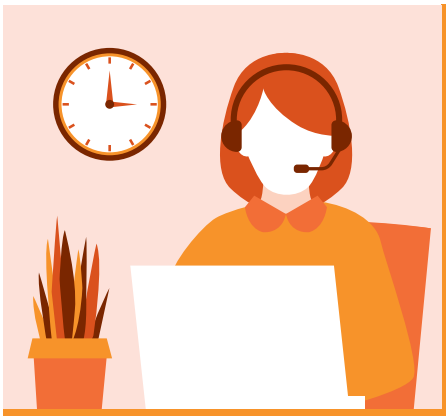
Persistent threats can last inside SME networks for years. Dwell time - the amount of time a threat spends inside of a network before an organisation discovers and removes it - has become a significant problem for SMEs, according to a U.S. report released by Infocyte in July 2019. Dwell time for attacks with ransomware averaged 43 days - and rose to 798 days for all other persistent threats (non-ransomware). Alarmingly, dwell time for riskware - defined as unwanted applications, web trackers, and adware - averaged a whopping 869 days.

The report stated that 72% of SMEs had riskware and unwanted applications in their networks that took longer than 90 days to remove. While they were generally lower risk issues, the bigger takeaway is networks that fail to control riskware typically have a lower readiness to respond to high-priority threats when they are uncovered.

The report advises that if continuous monitoring is not an option, SMEs should at the very least bring in a third-party to perform a compromise assessment.

Loss Mitigation Services

Some important loss mitigation services which are available to all of Chubb's cyber insurance customers include:



Incident Response Platform

Chubb offers customers an Incident Response Platform to help contain the threat and limit potential damage. It includes an on-call crisis response available 24/7/365 days; supported by contractual service level agreements. These agreements require a response within one hour from an incident manager and coordinated management of a team of experts to assist, manage and mitigate a wide array of cyber incident scenarios, including denial of service attacks, ransomware, cyber crime and employee error; and post-incident reporting. In the past 12 months, Chubb's average initial incident response time for customers in Asia Pacific was 12 minutes.

Phishing Assessments

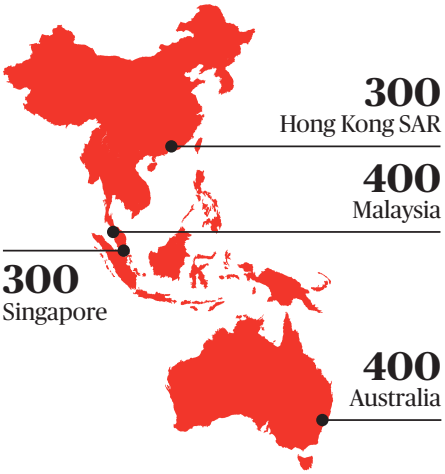
Chubb works with cyber phishing experts to offer phishing awareness assessments. The assessments include two simulated real-life phishing scenarios that are conducted over the course of four months, for up to 500 individual email addresses.

Complimentary Password Management

Remembering passwords is difficult. Companies can choose to use an all-in-one solution that remembers and automatically fills in user passwords and logins. With a secure sharing feature, colleagues can even share logins without ever seeing each other's passwords. Dark web monitoring can also help to scan the web and alert users immediately if their personal information is ever found where it doesn't belong online.

About the Research

This report is based on a survey of 1,400 respondents from Small and Medium Enterprises (SMEs) in four locations.



Respondents are from SMEs with 2 to 249 employees, and

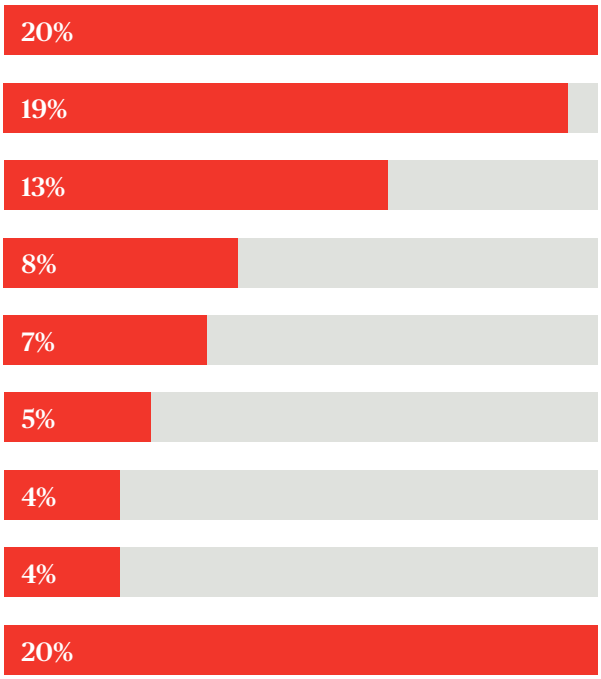
82%

Board-level executive

18%

Senior managers or directors below board level

The industries respondents belonged to are:



Practical steps SMEs can take to protect their business:

Develop and enforce a written password policy
Your employees will not thank you for forcing them to make passwords difficult to remember, but that's the point. Make them complicated (a combination of letters, numbers and symbols) and change them regularly. Disable access once employees leave the organisation.

Create a Cyber Incident Response Plan
45% of Singaporean SMEs admitted their current plan is ad-hoc and not documented. Of those that do have a plan in place, only 44% test it regularly. We recommend preparing a cyber incident response plan with the help of a cyber expert and conduct simulated tests on your plan regularly.

Educate employees regularly on cyber security vigilance
It only takes one click on a malicious link to expose a business to risk of a phishing or ransomware attack. Similarly, it only takes one call from "IT Support" to reveal passwords to cyber criminals.

Update IT equipment and deploy security software
Unpatched machines are much easier to access remotely, particularly if employees have elevated admin levels that they don't really need.

About Chubb in Singapore

Chubb is the world's largest publicly traded property and casualty insurer. Chubb Insurance Singapore Limited, via acquisitions by its predecessor companies, has been present in Singapore since 1948. Chubb in Singapore provides underwriting and risk management expertise for all major classes of general insurance. The company's product offerings include Financial Lines, Casualty, Property, Marine, Industry Practices as well as Group insurance solutions for large corporates, multinationals, small and medium-sized businesses. In addition, to meet the evolving needs of consumers, it also offers a suite of tailored Accident & Health and Personal & Specialty insurance options through a multitude of distribution channels including bancassurance, independent distribution partners and affinity partnerships.

Over the years, Chubb in Singapore has established strong client relationships by delivering responsive service, developing innovative products, and providing market leadership built on financial strength.

Contact Us

Chubb Insurance Singapore Limited
Co Regn. No.: 199702449H
138 Market Street
#11-01 CapitaGreen
Singapore 048946
O +65 6398 8000
F +65 6298 1055
www.chubb.com/sg

Chubb. Insured.™

Important Notes:

All content in this material is for general information purposes only. It does not constitute personal advice or a recommendation to any individual or business of any product or service.

Coverage are underwritten by one or more Chubb companies. Not all coverages are available in all countries and territories. Coverages are subject to licensing requirements and sanctions restrictions. This document is neither an offer nor a solicitation of insurance or reinsurance products.